Attacks/Breaches

1/8/2018
05:45 PM

Jai Vijayan
News

New Cryptocurrency Mining Malware Has Links to North Korea

A malware tool for stealthily installing software that mines the Monero virtual currency looks like the handiwork of North Korean threat actors, AlienVault says.

A security vendor has found another clue that North Korea may be turning to illegal cryptocurrency mining as a way to bring cash into the nation's economy amid tightening international sanctions.

AlienVault on Monday said it had recently discovered malware that is designed to stealthily install a miner for Monero, a Bitcoin-like cryptocurrency, on end-user systems and to send any mined coins to the Kim Il Sung University (KSU) in Pyongyang.

The malicious installer appears to have been created just before Christmas 2017 and is designed to install xmrig, an open source miner for Monero.

The link to the university itself doesn't appear to be working, however, meaning the software cannot send any mined coins back to its authors. The malware itself appears pretty basic, and the inclusion of the KSU server in the code could simply be a false flag to trick security researchers. Even so, the malware is consistent with previous similar campaigns tied to North Korea, AlienVault said.

"Cryptocurrencies could provide a financial lifeline to a country hit hard by sanctions," the vendor said. "Therefore it's not surprising that universities in North Korea have shown a clear interest in cryptocurrencies."

A cryptocurrency mining tool like xmrig is basically designed to harness the processing power of a computer in order to verify transactions in a blockchain. Users who put their computers to work mining virtual currencies such as Bitcoin and Monero typically receive small monetary rewards for allowing their hardware to be used for the purpose.

Crypto mining is legitimate activity. Some, like Coinhive, even distribute miners to website operators so users can run it in their browsers in exchange for an ad-free experience. In recent years, though, cybercriminals have increasingly begun hijacking computers in order to mine cryptocurrency for illegal profit.

In a report last September, IBM said that between January and July 2017 it had seen a six-fold increase in CPU mining attacks involving the use of malware for installing virtual currency mining tools against its customers. The tools typically were embedded in fake image files that were hosted on infiltrated servers running WordPress or

Joomla. Most of the attacks that IBM analyzed were designed to target virtual currencies such as Monero, whose CryptoNight algorithm can run on ordinary PCs and servers compared to the specialized hardware required for Bitcoin mining.

Last September, Kaspersky Lab reported finding two relatively large botnets comprised of computers infected with malware for installing legitimate cryptocurrency miners on them. The security vendor estimated that a 4,000-computer botnet used for cryptocurrency mining was netting its operators up to $30,000 a month, while a bigger 5,000-computer botnet was garnering its operators some $200,000 a month.

"As the price of crypto-currencies increase, so do the incentives to infect people with mining malware," says Chris Doman, security researcher at AlienVault. "Monero is becoming a popular choice as it is both more anonymous and more profitable to mine with malware."

Security researchers have found plenty of clues in recent months to suggest that Korea-linked threat actors like the Lazarus Group and others are actively engaged in cryptocurrency mining. Earlier this month, Bloomberg reported an incident in which a North Korea threat group called Andariel hijacked a server belonging to a South Korean organization and used it to mine about 70 Montero coins.

The Lazarus group has been caught doing Monero mining on compromised networks and attacking Bitcoin exchanges, Doman says. There have also been several public reports of North Korean universities looking into mining cryptocurrencies, Doman says. So while it is hard to say with complete certainty if the malware that AlienVault discovered is the work of North Korean actors, chances are high it is, he notes.

"The main takeaway for me is that this fits into the larger picture of North Korea and cryptocurrencies."

Related Content:

- **Cybercriminals Employ 'Driveby' Cryptocurrency Mining**
- **New 'Bondnet' Botnet Mines Cryptocurrencies**
- **Russian Developer Snuck Cryptocurrency Mining into Android Apps**
- **5 Reasons Why the CISO Is a Cryptocurrency Skeptic**

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year ... View Full Bio

8 Nation-State Hacking Groups to Watch in 2018

The Main AppSec Tech to Adopt in 2018

More White Papers

Reports

[Forrester's Report] The State of Application Security: 2018 & Beyond

[Strategic Security Report] Cloud Security's Changing Landscape

More Reports

Comments

Newest First | Oldest First | Threaded View

Be the first to post a comment regarding this story.

Sponsored by

Related Content

RESOURCES BLOG

Q2 Malware Review

Between the second quarter of 2017, PhishMe Intelligence completed analyses of 616 sets of phishing emails delivering ...

Enterprise Phishing Susceptibility Report

Phishing attacks remain the largest challenge to organizations because they target all employees.

Techniques for Dealing with Ransomware, BEC, and Spearphishing

IT decision makers across many industry verticals were surveyed on their experiences with phishing and malware ...

The Total Economic Impact of PhishMe's Human Phishing Defense

PhishMe recently commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the ...

Data Breaches and the Great Security Disconnect

The growing sophistication and fast-evolving nature of cyberthreats have made data breach preparedness a critical issue for enterprises.

Hot Topics **Editors' Choice**

5
Threats from Mobile Ransomware & Banking Malware Are Growing
Jai Vijayan, Freelance writer, 2/26/2018

2
Security Starts with the User Experience
Peter Hesse, Chief Security Officer at 10Pearls, 2/27/2018

1
SAML Flaw Lets Hackers Assume Users' Identities
Kelly Sheridan, Associate Editor, Dark Reading, 2/27/2018

Subscribe to Newsletters

Live Events Webinars

Why Hackers Attack: Understanding Threats & Motivations for Online Intrusion

Your Toughest AppSec Questions Answered

Cybersecurity Crash Course - Session 7: Security For IoT

Webinar Archives

White Papers

8 Nation-State Hacking Groups to Watch in 2018

Dark Reading Tech Digest: IT Skills Shortage

GDPR - Friend or Foe?

Minimze App Security Risks With DevOps

The Main AppSec Tech to Adopt in 2018

More White Papers

Video

How Security Metrics Fail **Attacking De**

All V os

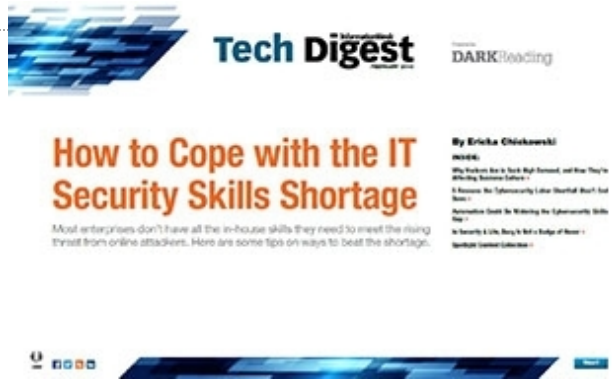
Cartoon Contest

Write a Caption, Win a Starbucks Card! Click Here

Latest Comment: I tried to tell him he was taking on too much.

Cartoon Archive

Current Issue



How to Cope with the IT Security Skills Shortage

Most enterprises don't have all the in-house skills they need to meet the rising threat from online attackers. Here are some tips on ways to beat the shortage.

Download This Issue!

Back Issues | Must Reads

Flash Poll

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

- Yes
- No
- No but we are considering it
- Still waiting for cybersecurity guidance from Trump admin EO
- Don't know

Other (Please explain in the comments)

Submit

All Polls

Reports

[Strategic Security Report] Navigating the Threat Intelligence Maze

Most enterprises are using threat intel services, but many are still figuring out how to use the data they're collecting. In this Dark Reading survey we give you a look at what they're doing today - and where they hope to go.

Download Now!

The State of Ransomware **0 comments**

[Strategic Security Report] How Enterprises Are Attacking the IT Security Problem **0 comments**

The Impact of a Security Breach 2017 **0 comments**

More Reports

Twitter Feed

Erik Nonaka @eneconsulting
New @Kaspersky #Spam and #Phishing #Report cites #banks, payment systems and #online #retail as top 3 phishing #threat targets of 2017 #netsec #cybersec via @DarkReading klab.so/78747F

15m

Martial Gervaise @argevise
Reviewing 8 #nationstate #hacker groups to keep an eye on in 2018 via our #cybersec expert #BrianBartholomew #turla #scarcruft #apt @kellysheridan @darkreading #NetSec #infosec kas.pr/3c15 via @kaspersky

1h

親孝行垢 Retweeted

ipfconline @ipfconline1
How Innovative Companies Lock Down Databuff.ly/2pO4Dzr by @JustinSomaini v/ @DarkReading#BigData #CyberSecurity #MachineLearning #Cognitive

Bug Report

Enterprise Vulnerabilities
From DHS/US-CERT's National Vulnerability Database

CVE-2017-0290
Published: 2017-05-09
NScript in mpengine in Microsoft Malware Protection Engine with Engine Version before 1.1.13704.0, as used in Windows Defender and other products, allows remote attackers to execute arbitrary code or cause a denial of service (type confusion and application crash) via crafted JavaScript code within ...

CVE-2016-10369
Published: 2017-05-08
unixsocket.c in lxterminal through 0.3.0 insecurely uses /tmp for a socket file, allowing a local user to cause a denial of service (preventing terminal launch), or possibly have other impact (bypassing terminal access control).

CVE-2016-8202
Published: 2017-05-08
A privilege escalation vulnerability in Brocade Fibre Channel SAN products running Brocade Fabric OS (FOS) releases earlier than v7.4.1d and v8.0.1b could allow an authenticated attacker to elevate the privileges of user accounts accessing the system via command line interface. With affected version...

CVE-2016-8209
Published: 2017-05-08
Improper checks for unusual or exceptional conditions in Brocade NetIron 05.8.00 and later releases up to and including 06.1.00, when the Management Module is continuously scanned on port 22, may allow attackers to cause a denial of service (crash and reload) of the management module.

CVE-2017-0890
Published: 2017-05-08
Nextcloud Server before 11.0.3 is vulnerable to an inadequate escaping leading to a XSS vulnerability in the search module. To be exploitable a user has to write or paste malicious content into the search dialogue.

Technology Group

Black Hat
Content Marketing Institute
Content Marketing World
Dark Reading
Enterprise Connect
GDC
Gamasutra
HDI
ICMI
InformationWeek
INsecurity
Interop ITX
Network Computing
No Jitter
Service Management World
VRDC

COMMUNITIES SERVED

Content Marketing
Enterprise IT
Enterprise Communications
Game Development
Information Security
IT Services & Support

WORKING WITH US

Advertising Contacts
Event Calendar
Tech Marketing
Solutions
Contact Us
Licensing